AMENDMENT TO THE CLAIMS

1. (Currently Amended). A system for user identity management and software product distribution comprising:

at least one authentication software product <u>embodied in a computer readable medium</u>; and

a security architecture software <u>embodied in a computer readable medium</u> capable of protecting the system;

wherein the at least one authentication software product is capable of servicing at least one external source<u>; and</u>

<u>wherein the authentication software product comprises an authentication device</u>.

2. (Currently Amended). The system of Claim 1 further comprising:

a profile application software <u>embodied in a computer readable medium</u> capable of maintaining an online electronic profile for each external source wherein the profile application software is accessible by external source system users and end users.

3. (Previously presented). The system of Claim 1 wherein the authentication software product comprises a series of platform-independent servlet based applications.

4. (Previously presented). The system of Claim 1 wherein the security architecture software is capable of automatic encoding of transmitted data using unique hashing routines.

5. (Previously presented). The system of Claim 1 wherein the security architecture software is capable of encrypting of transmitted data for security against spoofing.

6. (Previously presented). The system of Claim 1 wherein the system is capable of keeping track of each authentication software product devices and ownership/assignments to a plurality of external sources and their end users.

7. (Currently amended). The system of Claim 1 wherein the authentication software product comprises:

a username; and

a password; ~~and~~

~~an authentication device;~~

wherein the authentication device is selected from group consisting of software tokens, key chain tokens, and tokens capable of being read by a CD drive or Smart Card Reader.

8.   (Previously presented). An autonomous, stand-alone application using the system of Claim 1 wherein the authentication software product is capable of providing user authentication and access control as separate functions autonomous from the system of Claim 1.

9.   (Previously presented). The autonomous, stand-alone application using the system of Claim 8, wherein the at least one authentication software product and the security architecture software are capable of providing software piracy management to software manufacturers distributing application products via CD-ROM or a wide area network.

10.   (Previously presented). An autonomous application using the system of Claim 1, wherein the system is capable of being deployed completely on a client's site, wherein the client comprises a client server, in which the client server is capable of functioning as a server application independent of the system of Claim 1.

11.   (Original). The system of Claim 1 wherein the system is capable of reading CD-ROM content remotely via a wide area network.

12.   (Original). The system of Claim 1 wherein the system is capable of providing CD media-based copy protection and is capable of validating the CD media.

13.   (Original). The system of Claim 1 wherein the system is capable of providing CD media authentication remotely via a wide area network.

14.   (Original). The system of Claim 1 wherein the system is capable of providing embedded, encrypted serialization of CD media.

15.   (Original). The system of Claim 1 wherein the system is capable of providing anti-piracy protection to electronically distributed software.

16.   (Original). The system of Claim 1 wherein the system is capable of using CD media developed with anti-piracy technology as effective user authentication devices.

17.   (Original). The system of Claim 1 wherein the system is capable of bundling any combination of full products, limited-use versions, trial versions, demo versions, and license packs on at least one CD-ROM.

18.   (Original). The system of Claim 1 wherein the system is capable of managing and tracking specific and group end-user access authorizations to digital content and processes for each external source.